

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Délégué à la protection des données

Rosier, Karen

Published in:

Le règlement général sur la protection des données (RGPD/GDPR)

Publication date:

2018

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Rosier, K 2018, Délégué à la protection des données: une fonction multifacette. Dans *Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie*. Cahiers du CRIDS, Numéro 44, Larcier , Bruxelles, p. 559-592.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

TITRE 10

Délégué à la protection des données : une fonction multifacette¹

Karen ROSIER²

CHAPITRE 1. Pourquoi un délégué à la protection des données ?

1. La figure de délégué à la protection des données n'est pas nouvelle. L'article 18 de la directive 95/46/CE³ (ci-après, la « Directive ») prévoyait la possibilité pour le responsable du traitement de désigner un détaché à la protection des données à caractère personnel. Les États membres pouvaient ainsi prévoir une simplification de la notification de traitement à l'autorité de contrôle ou une dérogation à cette obligation lorsque le responsable du traitement avait désigné, conformément au droit national auquel il est soumis, un détaché à la protection des données à caractère personnel. Plusieurs États membres ont fait usage de cette possibilité et la notion de délégué à la protection des données avait, par ailleurs, été instituée au sein du règlement (CE) 45/2001⁴.

¹ Cette contribution est une version légèrement remaniée et actualisée d'un texte publié sous l'intitulé « Délégué à la protection des données. Une nouvelle fonction, un métier en devenir », in *Vers un droit européen de la protection des données ?*, coll. UB3, Bruxelles, Larcier, 2017, pp. 135-168.

² Maître de conférences à l'Université de Namur, chercheuse au Centre de Recherche Information, Droit et Société (CRIDS), Université de Namur et avocate (Versius).

³ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

⁴ Règlement (CE) 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

2. Ce qui est nouveau en revanche, c'est que le règlement général sur la protection des données (ci-après, le « RGPD »)⁵ rend obligatoire la désignation d'un tel délégué dans certains cas de figure et que cette obligation peut concerner tant le responsable du traitement que le sous-traitant. Nous le verrons, de nombreux responsables du traitement et sous-traitants seront désormais potentiellement concernés par cette obligation nouvelle pour eux. Nul besoin non plus de transposition en droit national pour activer cette obligation puisque le régime de désignation est prévu directement au sein du RGPD, dont l'entrée application sur tout le territoire de l'Union a été fixée au 25 mai 2018.

3. Le RGPD esquisse en quelques articles les hypothèses dans lesquelles la désignation du délégué à la protection des données (ou en anglais, « DPO » pour « *data protection officer* ») est obligatoire, son profil et ses fonctions ainsi que les principaux aspects des conditions dans lesquelles il doit exécuter sa mission⁶. Le texte du RGPD demeure donc relativement succinct. Le Groupe 29 avait annoncé que, dans la perspective de la transition et de la préparation à la mise en œuvre du RGPD, il avait l'intention d'émettre des directives, notamment sur la question du délégué à la protection des données⁷. Cela a été chose faite avec la publication d'un premier texte du 13 décembre 2016, amendé et finalement adopté le 5 avril 2017⁸ qui contient effectivement de précieuses lignes directrices en ce qui concerne la mise en œuvre de ces quelques dispositions du RGPD (ci-après, les « Lignes directrices »)⁹. Ces Lignes directrices donnent une contenance plus concrète aux dispositions de la réglementation et permettent de mieux entrevoir dans quel sens il faut comprendre ces dispositions.

4. Le Groupe 29 évoque le délégué à la protection des données comme un « facilitateur ». Facilitateur, d'abord, pour assurer la mise en œuvre du respect de la réglementation au sein des organisations des responsables du traitement et des sous-traitants. Facilitateur, ensuite, parce qu'il est censé transmettre l'information, tant au sein de l'entreprise ou de l'autorité

⁵ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD).

⁶ Art. 37, 38 et 39 du RGPD.

⁷ Groupe 29, Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR), WP 236, 2 février 2016.

⁸ Groupe 29, Guidelines on data protection officers, WP 243 rev. 01, adopté le 13 décembre 2016 et révisé le 5 avril 2017, ci-après les « Lignes directrices ».

⁹ Il a annoncé que d'autres directives pourraient être émises afin de donner plus de précisions lorsque cela s'avèrera utile (Lignes directrices [voy. *supra*, note n° 7], p. 5).

concernée, entre les différents départements de celle-ci, que vis-à-vis des personnes concernées et des autorités de contrôle¹⁰.

La dynamique voulue par le RGPD est, selon le Groupe 29, que le délégué à la protection des données n'est pas responsable du respect de la législation. Cette responsabilité incombe uniquement au responsable du traitement ou au sous-traitant. La désignation d'un délégué est d'ailleurs étroitement liée au principe d'« *accountability* » qui est l'un des axes importants du RGPD. Ce principe d'« *accountability* » affirmé à l'article 5, paragraphe 2, du RGPD vient appuyer les autres principes clés de la réglementation¹¹. Le responsable du traitement, comme sous le régime de la Directive, est tenu de respecter les principes fondamentaux applicables à tout traitement, mais il est désormais spécifié qu'il doit démontrer que ceux-ci sont respectés¹². C'est ce que désigne ce « principe de responsabilité » entendu non pas comme impliquant essentiellement une obligation de réparer le dommage en cas de violation de la réglementation¹³, mais davantage comme l'idée qu'il convient de « répondre de », en l'occurrence répondre des mesures prises pour assurer le respect du RGPD (le concept étant mieux traduit par le terme anglais d'« *accountability* », distinct de celui de « *liability* » qui subsiste par ailleurs). Cela suppose donc une certaine proactivité et anticipation des critiques que l'on pourrait formuler à l'égard d'un traitement et la prise de mesures anticipatives pour assurer le respect de celui-ci. Ce principe général d'« *accountability* » applicable à tout traitement prend corps avec des obligations particulières pour certains types de traitements ou responsables du traitement, qui formalisent les mesures à prendre par le responsable du traitement pour s'assurer du respect des principes de protection. Parmi ces mesures, il en est une, de nature organisationnelle, qui est de nommer un délégué à la protection des données.

Cette mesure est également mise à charge du sous-traitant qui, bien que n'ayant pas à proprement parler les mêmes obligations que le responsable du traitement, doit mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer qu'il respecte les obligations qui lui incombent en vertu de l'article 28 du RGPD¹⁴.

¹⁰ *Ibid.*, p. 4.

¹¹ Définis à l'article 5, § 1^{er}, du RGPD. Pour une contribution présentant le RGPD, voy. C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Les lignes de force du nouveau RGPD relatif à la protection des données à caractère personnel », *R.D.T.I.*, n° 62, 2016, pp. 5 et s. (certains passages de la présente contribution reproduisent une partie de ce texte).

¹² Art. 5, § 2, du RGPD.

¹³ Comp. avec l'article 23 de la Directive intitulé « responsabilité ».

¹⁴ Art. 28, § 3, h), du RGPD.

5. Obligatoire dans certains cas, la désignation d'un délégué à la protection des données est encouragée par le Groupe 29 dans les hypothèses où cela ne l'est pas¹⁵. Le Groupe 29 signale encore que désigner un délégué à la protection des données n'est qu'une première étape mais que le responsable ou sous-traitant doit donner au délégué à la protection des données suffisamment d'autonomie et de ressources pour pouvoir effectivement exercer les tâches qui lui incombent¹⁶. Il insiste sur le rôle crucial que doit jouer le responsable du traitement ou le sous-traitant dans la facilitation de l'exercice des compétences du délégué à la protection des données.

6. Nous nous proposons dans le cadre de la présente contribution de fournir une analyse des dispositions du RGPD concernant le délégué à la protection des données à la lumière des Lignes directrices.

CHAPITRE 2. Un délégué à la protection des données pour qui ?

SECTION 1. – Les hypothèses de désignation prévues dans le RGPD

7. Tout responsable du traitement ou sous-traitant peut désigner un délégué à la protection des données, ce qui entraînera alors l'application du RGPD audit délégué, notamment en ce qui concerne les protections contre un licenciement ou une rupture de contrat¹⁷. Nous y reviendrons¹⁸.

Dans certains cas, il devra en tout état de cause le faire. Les hypothèses visées par le RGPD s'articulent autour de conditions d'application de plusieurs ordres : d'une part, la qualité d'autorité publique ou d'organisme public du responsable du traitement ou du sous-traitant concerné et, d'autre part, l'activité concernée, combinée ou non à la nature des données traitées.

¹⁵ Lignes directrices (voy. *supra*, note n° 7), p. 4.

¹⁶ Lignes directrices (voy. *supra*, note n° 7), p. 4.

¹⁷ Art. 37, §§ 1^{er} et 4, du RGPD. Se posera donc la question de la qualification de la fonction qui sera dévolue à un juriste chargé des aspects protection de données au sein d'une entreprise qui n'est pas tenue de désigner un délégué à la protection des données dès lors que la qualité de délégué à la protection des données entraîne une série de garanties et d'obligations vis-à-vis de ce dernier qui sont prévues dans le RGPD.

¹⁸ Voy. Chapitre 4, Section 3, *infra*.

§ 1. Hypothèse liée à la qualité du responsable du traitement ou du sous-traitant

8. Il s'agit tout d'abord des traitements effectués par une autorité publique ou un organisme public, exception faite toutefois des juridictions agissant dans l'exercice de leur fonction juridictionnelle¹⁹.

Les notions d'autorité publique et d'organisme public ne sont pas définies dans le RGPD. Le Groupe 29 considère que le concept d'autorité publique ou d'organisme public devra être déterminé en fonction de la loi nationale²⁰. Il relève que cela peut concerner les autorités ou organisations publiques au niveau national, régional ou plus local mais également, selon ce que prévoit le droit national, toute une série d'entreprises ou d'organisations qui appartiennent au secteur privé mais qui exercent des activités relevant d'une mission publique, telles que des entreprises assurant les transports publics, la fourniture d'énergie ou d'eau, les infrastructures routières, un service de radiodiffusion ou encore des ordres professionnels exerçant des missions disciplinaires²¹.

Seule la qualité d'autorité publique ou d'organisme public compte pour déterminer si oui non la désignation d'un délégué à la protection des données est requise. Il ne s'agit donc pas d'une obligation de portée fonctionnelle. *A priori*, les missions du délégué couvriront tous les traitements de données effectués par le sous-traitant ou le responsable du traitement concerné sans être limitées à ce qui entre strictement dans l'exercice d'une partie de la puissance publique²². Ainsi le délégué à la protection des données de l'employeur du secteur public exercera les missions qui lui sont dévolues pour ce qui concerne le traitement des données des fonctionnaires au service de l'autorité ou de l'organisme concerné.

Notons toutefois que le Groupe 29 recommande la désignation d'un délégué à la protection des données dans le chef des entreprises ou organismes privés qui exercent des missions publiques ou des tâches de services publics en s'appuyant sur le constat selon lequel dans un tel cas de figure les personnes concernées se trouvent dans une situation assez similaire à celle dans laquelle l'autorité publique traite elle-même les données²³.

¹⁹ Art. 37, § 1^{er}, a).

²⁰ Lignes directrices (voy. *supra*, note n° 7), p. 6.

²¹ *Ibid.*

²² Lignes directrices (voy. *supra*, note n° 7), p. 6.

²³ Par exemple, le traitement se fait sans le consentement des personnes ou moyennant une information réduite (voy. V. VERBRUGGEN, « Mise en œuvre du Règlement général sur la protection des données : coup de projecteur sur certaines nouvelles obligations à charge des responsables de traitement ou des sous-traitants », *Orientations*, 2017/5, p. 18.

9. Pour ce qui est de l'exception prévue pour les juridictions, le considérant n° 97 du RGPD ajoute qu'il s'agit des juridictions agissant dans l'exercice de leur fonction juridictionnelle. Telle que libellée cette exception paraît ne viser que les traitements strictement limités à l'exercice de la fonction juridictionnelle mais n'englobe pas nécessairement les traitements liés à l'administration du personnel d'une juridiction.

Cela revient à considérer que, pour ce qui concerne les traitements de données strictement liés à la fonction de juger, les juridictions ne doivent pas s'adjoindre de délégué à la protection des données. À nouveau, on peut supposer qu'il y aura lieu de se référer au droit national pour déterminer quelles sont les autorités visées. On notera que le considérant n° 97 évoque les juridictions indépendantes ainsi que les *autorités judiciaires indépendantes*, sans que cette dernière notion ne soit définie ni reprise dans le texte de l'article 37 du RGPD. Cela laisse entendre toutefois qu'une interprétation assez large des personnes visées par l'exception est concevable, par exemple en ne la limitant pas aux magistrats mais également à tous les organes qui participent à la fonction de juger.

§ 2. Hypothèses liées à l'activité du responsable du traitement ou du sous-traitant

10. Pour le secteur privé, la désignation d'un délégué à la protection des données sera requise lorsque les activités de base du responsable du traitement ou du sous-traitant²⁴ consistent (i) en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ou encore (ii) en un traitement à grande échelle de données sensibles²⁵ ou ²⁶ judiciaires²⁷.

²⁴ Cette référence aux « activités de base du responsable » implique, *a contrario*, que lorsque les traitements ne sont effectués qu'au soutien d'une activité auxiliaire du responsable, ils ne donnent pas lieu à l'obligation de désigner un DPO.

²⁵ Entendues comme les données visées à l'article 9 du RGPD.

²⁶ Le texte du RGPD énonce que des « activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ». Toutefois, comme le relève le Groupe 29 à propos l'usage de la conjonction « et », il n'y a pas de raison d'exiger les traitements des deux catégories d'informations de sorte qu'il convient de lire le texte comme « ou » (Lignes directrices [voy. *supra*, note n° 7], p. 9). Un rectificatif du RGPD a d'ailleurs opéré cette modification de lien de coordination (Rectificatif du règlement (UE) 2016/679, JOUE, L127/2, 23 mai 2018).

²⁷ Art. 37, § 1^{er}, a) et b), et considérant n° 97 du RGPD.

a) Sur la notion d'activité de base

11. Il est question dans les deux cas d'examiner les activités de base du responsable du traitement ou du sous-traitant. Le considérant n° 97 oppose cette notion à celle de « traitement des données à caractère personnel en tant qu'activité auxiliaire ».

Le Groupe 29 fournit, sur ces notions d'activité principale et auxiliaire, des éclaircissements tout à fait essentiels. En effet, une première lecture de ces dispositions jette le doute sur la façon dont il convient d'interpréter l'article 37 du RGPD. Vu l'informatisation des acteurs économiques, la plupart des responsables de traitements mène leurs activités principales en réalisant des traitements de données. Quelle entreprise ne compte pas de fichiers clients, de données informatisées concernant son personnel, ses prospects ?

12. Le Groupe 29 précise que doivent être considérées comme « activités de base » d'une organisation toutes activités de traitement de données qui forment une part inextricable de l'activité du responsable du traitement ou du sous-traitant. Il ne s'agit donc pas de s'intéresser uniquement au type de services que fournit cette personne mais de vérifier si, lorsqu'elle fournit ces services, cela passe par un traitement de données qui ne peut être détaché de la fourniture de ces services²⁸.

Un exemple donné par le Groupe 29 est celui des hôpitaux : le suivi médical d'un patient passe par des traitements d'informations relatives à sa santé. On ne peut donc pas séparer le service de soins fourni par un hôpital des traitements de données qui y sont liés²⁹.

Il nous semble que, dans le même sens, les traitements de données qui sont effectués par les organismes bancaires font partie de son activité de base puisque les services bancaires se fondent sur un traitement de l'information relatif aux mouvements de compte, aux crédits, etc. accordés et qui sont largement liés à des traitements de données à caractère personnel.

À la différence, une activité de vente en grande surface ne repose pas sur le traitement de données à caractère personnel. L'entreprise traite sans doute des données à caractère personnel concernant ses fournisseurs ou des clients, mais son activité n'est pas inextricablement liée à ces traitements. La situation est différente nous semble-t-il si ce commerce a lieu dans un environnement numérique, dans le cadre d'une plateforme de

²⁸ Lignes directrices (voy. *supra*, note n° 7), p. 7.

²⁹ *Ibid.*

commerce électronique. Dans un tel contexte, le déroulement de l'activité repose sur le traitement de données de la clientèle.

Seraient dès lors exclus des traitements de l'activité de base de l'entreprise, les traitements de données qui sont liés à l'informatisation du fonctionnement d'une entreprise mais qui ne sont pas liés au service lui-même, par exemple le fait qu'une entreprise commerciale dispose d'un serveur, d'un programme comptable ou d'un système de *back up* de données à caractère personnel n'implique pas qu'il s'agisse d'une activité principale. Il s'agit bien d'un aspect auxiliaire de son activité, même si cela permet d'effectuer des traitements de données³⁰.

13. Il faudra donc se poser la question de savoir si le service ou l'activité du sous-traitant ou du responsable du traitement repose sur des traitements de données à caractère personnel ou si les traitements de données à caractère personnel qui sont effectués par l'entreprise s'expliquent uniquement par l'informatisation du traitement de l'information au sein de celle-ci sans que cela ne soit absolument nécessaire à la prestation des services.

b) Sur la notion de traitement « à grande échelle »

14. La notion de traitement à grande échelle n'est pas définie. Elle est évoquée notamment à propos de l'obligation d'effectuer une analyse de risque préalablement à la mise en œuvre d'un traitement. Le considérant n° 91 du RGPD laisse entendre dans ce contexte qu'un traitement à grande échelle vise à traiter un volume « considérable » de données à caractère personnel au niveau régional, national ou infranational. Il précise que ne devrait pas être considéré comme étant à grande échelle, le traitement qui concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. Cette précision est d'un intérêt limité puisque, si on peut imaginer qu'un avocat ou un médecin exerçant seul n'opère habituellement pas de traitement à grande échelle, il y a toute une gamme de situations pour lesquelles il reste une grande marge d'appréciation. On peut par exemple se demander si une association comptant quinze personnes sera considérée comme mettant en œuvre des traitements à grande échelle. Il y a donc une incertitude juridique à notre sens sur la manière dont il faut apprécier la portée du concept de « traitement à grande échelle » au cas par cas, sans que l'on sache où la barre du volume « considérable » de données doit être placée.

³⁰ Lignes directrices (voy. *supra*, note n° 7), pp. 7-8.

Le Groupe 29 fournit des indicateurs complémentaires pour apprécier si oui ou non le traitement est à grande échelle :

- le nombre de personnes concernées, que ce soit sous l’angle d’un nombre spécifique ou d’une proportion par rapport à une population déterminée ;
- le volume de données ou le nombre de données différentes qui est traité ;
- la durée de traitement, ou encore son caractère permanent ou non ;
- l’étendue territoriale de l’activité de traitement³¹.

Il cite notamment comme exemple de traitement à grande échelle le traitement de données relatives à des patients dans le cadre de l’activité normale d’un hôpital, le traitement des données relatives au transport pour une société de transport public (par exemple via des cartes à puce de transport public), ou encore le traitement de données de la clientèle par une banque ou une compagnie d’assurance³².

On en retient qu’il n’y a donc pas de chiffre déterminé qui permet de faire la ligne de partage entre ce qui constitue un traitement à grande échelle et ce qui ne le constitue pas. Tout est question d’appréciation au cas par cas, d’où l’utilité, comme l’indique le Groupe 29, de pouvoir documenter une réflexion à cet égard lorsqu’un responsable du traitement considère qu’il n’entre pas dans son obligation de désigner un délégué à la protection des données eu égard au fait qu’il estime ne pas traiter des données à grande échelle³³.

c) Sur la notion « de suivi régulier et systématique »

15. En ce qui concerne la notion de « traitement régulier et systématique », elle n’est, à nouveau, pas définie dans le RGPD et n’est évoquée indirectement que par rapport à un autre aspect de la réglementation – son champ d’application territorial – au considérant n° 24. Le Groupe 29 précise que si cette notion implique très clairement les activités de *tracking* ou de profilage sur internet comme mentionné dans ce considérant, sa portée ne s’y limite pas, ni ne se restreint à l’environnement numérique³⁴.

Selon le Groupe, il convient de considérer qu’il y a suivi régulier lorsqu’un suivi (1) soit intervient à des intervalles particuliers sur une période donnée, (2) soit est réalisé de façon récurrente et répétitive à certains moments ou (3) encore est effectué de façon constante ou de façon périodique.

³¹ Lignes directrices (voy. *supra*, note n° 7), p. 7.

³² Lignes directrices (voy. *supra*, note n° 7), p. 8.

³³ Lignes directrices (voy. *supra*, note n° 7), p. 5.

³⁴ Lignes directrices (voy. *supra*, note n° 7), p. 8.

Pour ce qui est de la notion de systématique, le Groupe 29 considère qu'il faut avoir égard au fait que (1) le traitement intervient en exécution d'un système, ou (2) qu'il intervient de façon préétablie, organisée ou méthodique, (3) qu'il prend place dans une planification générale de la collecte d'information ou encore (4) qu'il s'inscrit dans une stratégie³⁵.

Le Groupe 29 fournit différents exemples qui permettent de cerner les hypothèses dans lesquelles ces deux conditions sont rencontrées³⁶. Sont notamment mises en exergue dans ces exemples les pratiques suivantes :

- le profilage, que ce soit à des fins de publicité comportementale ou d'évaluation de risques notamment dans les secteurs des assurances ou du crédit ou de la détection du blanchiment d'argent ;
- la géolocalisation systématique, par exemple par le biais d'applications mobiles ;
- la surveillance qui implique une collecte régulière d'informations (par exemple dans le cadre d'un suivi de la santé via des terminaux mobiles, ou de la vidéosurveillance) ;
- la prestation de services reposant sur des systèmes automatisés connectés (objets connectés).

SECTION 2. – Possibilité d'imposer la désignation d'un délégué dans d'autres cas de figure

16. Le RGPD laisse aux États membres ou au droit de l'Union la possibilité d'imposer la désignation d'un délégué dans d'autres hypothèses³⁷. Dans une version intermédiaire de la proposition de RGPD³⁸, l'obligation de désigner un délégué à la protection des données était d'ailleurs entièrement laissée à la discrétion des États membres, avant que ne soient réintroduits les cas de figure spécifiques qui ont été évoqués dans les précédentes sections.

En droit belge, il avait par exemple été fait obligation jusqu'à présent de désigner un « conseiller en sécurité de l'information » notamment aux participants au système d'échanges de données administratives (registre

³⁵ Lignes directrices (voy. *supra*, note n° 7), p. 8.

³⁶ Lignes directrices (voy. *supra*, note n° 7), p. 9.

³⁷ Art. 37, § 4, du RGPD.

³⁸ Art. 35 de la version consolidée du 11 juin 2015 de la Proposition de RGPD après la réunion du Coreper du 9 juin 2015 (<http://data.consilium.europa.eu/doc/document/ST-9788-2015-INIT/en/pdf>).

national, banque de la sécurité sociale, etc.)³⁹ et dans des activités liées au secteur public⁴⁰ et de la santé⁴¹.

SECTION 3. – Qui du responsable du traitement ou du sous-traitant doit désigner un délégué à la protection des données ?

17. Le libellé de l'article 37 du RGPD formule l'obligation de désigner un délégué à la protection des données à charge du responsable du traitement et du sous-traitant dans les trois hypothèses qu'il prévoit et que nous venons d'évoquer. Est-ce à dire que chacun d'eux devra le faire dès lors que seul le responsable ou le sous-traitant se trouve concerné par une de ces hypothèses ? Il ne nous semble pas que cette interprétation soit compatible avec la philosophie de la disposition. Si l'idée est d'imposer l'intervention d'un délégué en raison de l'appartenance au secteur public ou de traitements liés à une activité de base, il nous apparaît que l'obligation est propre au sous-traitant ou au responsable selon son appartenance ou non au secteur public, ou selon les particularités de ses activités s'il s'agit d'une organisation relevant du secteur privé. Cette interprétation est confirmée par le Groupe 29 qui indique que ce n'est pas parce qu'un responsable du traitement devrait désigner un délégué à la protection des données au regard des critères définis par le règlement que son sous-traitant devrait le faire⁴².

Il convient donc d'envisager la situation de l'un et de l'autre séparément, bien que le Groupe 29 relève que cela pourrait être une bonne pratique lorsque le responsable du traitement doit désigner un délégué à la protection des données, que son sous-traitant en fasse autant⁴³.

Ainsi, si une société du secteur privé se spécialise dans l'hébergement de données de cabinets médicaux et effectue de ce fait des opérations sur

³⁹ Voy. not. le système institué par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral.

⁴⁰ Voy. égal. la fonction de conseillers en sécurité et en protection de la vie privée créée dans les zones de police (Arrêté royal du 6 décembre 2015 relatif aux conseillers en sécurité et en protection de la vie privée et à la plate-forme de la sécurité et de la protection des données) et à ce sujet : E. DEGRAVE, « La protection des données à caractère personnel enfin réformée », *JDE*, 2016, p. 136.

⁴¹ Art. 24 de la loi du 5 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale ; arrêté royal du 3 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre (annexe A).

⁴² Lignes directrices (voy. *supra*, note n° 7), p. 9.

⁴³ *Ibid.*

de nombreuses données provenant de différents responsables du traitement, elle devrait désigner un délégué à la protection de données. Tel ne devrait pas être le cas pour le médecin responsable du traitement qui exerce à titre individuel et fait appel à ce prestataire pour héberger les données liées à cette activité.

18. Le Groupe 29 recommande également que, lorsqu'un délégué à la protection des données est désigné pour encadrer des traitements de données qui sont mis en œuvre par un sous-traitant en sa qualité de sous-traitant, ce délégué supervise aussi le traitement des données effectué par ce sous-traitant en qualité de responsable de traitement, par exemple par rapport aux données qu'il traite dans le cadre de ses relations avec ses clients ou ses employés ou ses fournisseurs⁴⁴.

SECTION 4. – Quelles conséquences en cas de désignation d'un délégué dans des cas où il n'y pas d'obligation de le faire ?

19. Une organisation qui n'a pas l'obligation légale de désigner un délégué à la protection des données est libre de le faire et est même encouragée en ce sens par le Groupe 29 au titre de bonne pratique organisationnelle. Si la décision de désigner un délégué à la protection des données peut être motivée par l'intérêt de pouvoir démontrer un certain engagement dans la voie du respect de la législation en matière de protection des données, cela n'entraîne pas, au regard du RGPD d'autres avantages, telle qu'une dispense ou une facilitation dans l'accomplissement de certaines démarches (comme c'était le cas sous l'égide de la Directive pour ce qui concernait les notifications de traitement). Nous n'identifions qu'une disposition spécifique évoquée à l'article 57, paragraphe 3, du RGPD, mais dont on ne mesure pas encore la portée concrète. Cette disposition prévoit que « l'accomplissement des missions de chaque autorité de contrôle est gratuit pour la personne concernée et, le cas échéant, pour le délégué à la protection des données ».

Dans l'hypothèse où un responsable du traitement ou un sous-traitant désigne, sans y être légalement tenu, un délégué à la protection des données, le statut de délégué avec les obligations et protections y associées s'appliqueront à l'instar d'un délégué à la protection des données qui a été désigné en vertu d'une obligation légale⁴⁵.

⁴⁴ Lignes directrices (voy. *supra*, note n° 7), p. 10.

⁴⁵ Lignes directrices (voy. *supra*, note n° 7), p. 5.

SECTION 5. – Exercice de la fonction de délégué à la protection des données pour plusieurs entités

20. Le RGPD prévoit des hypothèses dans lesquelles plusieurs entités peuvent désigner une même personne en qualité de délégué à la protection des données, ces entités mutualisant ainsi cette ressource.

Ainsi un groupe d'entreprises peut-il nommer un seul délégué à la protection des données⁴⁶. La notion de groupe d'entreprises désigne une entreprise et celles sur lesquelles elle exerce le contrôle⁴⁷. Il s'agit donc de cas assez spécifiques puisque les entreprises concernées ont un lien entre elles.

La condition posée dans le RGPD est que le délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement. Commentant cette disposition, le Groupe 29 a interprété cette condition comme impliquant que le délégué soit occupé sur le territoire de l'Union européenne, même si le responsable du traitement ou le sous-traitant qui l'a désigné est établi hors de ce territoire. Le Groupe concède toutefois qu'il peut être dérogé à cette règle si le responsable ou le sous-traitant n'a aucun établissement sur le territoire européen⁴⁸.

21. Le Groupe 29 ajoute que ce délégué à la protection des données doit pouvoir effectivement être contacté dans la langue d'usage des personnes concernées et de l'autorité de contrôle. La communication des données de contact doit précisément permettre cette communication⁴⁹. Ces préoccupations du Groupe 29 qui ajoutent en réalité d'autres conditions pratiques sont compréhensibles. Si un seul délégué représente plusieurs entités situées sur des territoires, le cas échéant de langues différentes, il doit être à même d'exercer une des compétences qui lui sont dévolues, à savoir de pouvoir communiquer avec toutes les autorités de contrôle concernées et des personnes concernées issues de ces différents territoires. Il ne s'agit pas seulement de savoir comment contacter ce délégué mais d'être assuré de pouvoir communiquer avec lui.

⁴⁶ Art. 37, § 2, du RGPD.

⁴⁷ Art. 4, 19), du RGPD. Le considérant n° 37 précise encore à cet égard que « Un groupe d'entreprises devrait couvrir une entreprise qui exerce le contrôle et ses entreprises contrôlées, la première devant être celle qui peut exercer une influence dominante sur les autres entreprises du fait, par exemple, de la détention du capital, d'une participation financière ou des règles qui la régissent, ou du pouvoir de faire appliquer les règles relatives à la protection des données à caractère personnel. Une entreprise qui contrôle le traitement de données à caractère personnel dans des entreprises qui lui sont affiliées devrait être considérée comme formant avec ces dernières un groupe d'entreprises ».

⁴⁸ Lignes directrices (voy. *supra*, note n° 7), p. 11.

⁴⁹ Lignes directrices (voy. *supra*, note n° 7), p. 11.

Une seconde hypothèse dans laquelle un délégué peut être désigné pour plusieurs entités est prévue dans le RGPD pour le secteur public. Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type⁵⁰. Il s'agit donc d'une possibilité mais qui doit toutefois tenir compte de la charge de travail effective que cela représente pour le délégué pressenti, eu égard par exemple à l'ampleur des activités et traitements concernés⁵¹.

22. Notons encore que le RGPD prévoit, hors des hypothèses où une désignation d'un délégué à la protection des données est obligatoire, que des associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, doivent désigner un délégué à la protection des données qui pourra agir pour ces associations et autres organismes⁵².

23. Il est d'autres hypothèses, non envisagées spécifiquement dans le RGPD, où nous semble-t-il une même personne pourrait endosser la fonction de délégué à la protection des données. En effet, nous verrons que le Groupe 29 estime que la fonction de délégué à la protection des données pourrait être exercée par une personne morale, telle par exemple un cabinet de consultance. Il s'agira alors de désigner une personne physique responsable, le cas échéant au sein d'une équipe de plusieurs personnes assumant les tâches dévolues au délégué à la protection des données. Dans un tel cas de figure, la charge de travail concrète que peut assumer le délégué prend un autre visage dans la mesure où le travail est réparti sur plusieurs têtes avec éventuellement des compétences linguistiques également démultipliées. Rien n'empêche qu'un consultant externe, le cas échéant personne morale, puisse être désigné par des responsables du traitement ou sous-traitants distincts qui n'ont aucun lien entre eux. Se posera néanmoins éventuellement la question de conflits d'intérêts sur laquelle nous reviendrons⁵³.

⁵⁰ Art. 37, § 3, du RGPD.

⁵¹ Lignes directrices (voy. *supra*, note n° 7), p. 11.

⁵² Art. 37, § 4, du RGPD.

⁵³ Voy. *infra*, Chapitre 3, Section 2.

SECTION 6. – Incidence d’une application extraterritoriale du RGPD

24. De par les critères d’application du RGPD, il n’est pas exclu qu’un délégué à la protection des données doive être désigné par une société établie en dehors du territoire de l’Union.

En effet, le règlement adopte de nouveaux critères liés à la localisation du public cible du traitement de données pour s’appliquer aux responsables du traitement établis hors de l’Union européenne. Sans doute inspirés par une volonté de réagir aux collectes et traitements à grande échelle de données de résidents européens par des sociétés établies en dehors de l’Union, deux nouveaux critères sont insérés à l’article 3 du RGPD pour rendre ce dernier applicable à des responsables de traitement non établis sur le territoire européen. Il est désormais prévu que le « règlement s’applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l’Union par un responsable du traitement ou un sous-traitant qui n’est pas établi dans l’Union, lorsque les activités de traitement sont liées : a) à l’offre de biens ou de services à ces personnes concernées dans l’Union, qu’un paiement soit exigé ou non desdites personnes ; ou b) au suivi du comportement de ces personnes, dans la mesure où il s’agit d’un comportement qui a lieu au sein de l’Union ».

Ces deux critères ont en commun de déplacer la question de la localisation des moyens de traitement vers celle de la localisation du public cible du traitement des données. Des responsables du traitement ou sous-traitants établis hors du territoire européen peuvent être amenés à désigner un délégué à la protection des données auquel s’appliquera le régime du RGPD.

Une particularité de leur situation provient du fait que le responsable du traitement ou le sous-traitant concerné doit par ailleurs désigner un représentant. Le représentant sera l’interlocuteur à qui devront s’adresser les autorités de contrôle et les personnes concernées et il devra répondre vis-à-vis d’eux du respect des obligations du responsable du traitement ou du sous-traitant qui l’aura désigné par écrit en cette qualité⁵⁴. Or nous le verrons, une des missions du délégué à la protection des données est de servir de point de contact pour les autorités de contrôle⁵⁵. Il y a donc une forme de potentielle « concurrence » entre le représentant et le délégué à la protection des données sur ce point, sachant que le RGPD n’impose

⁵⁴ Art. 27, § 3, du RGPD.

⁵⁵ Art. 39, § 1^{er}, e), du RGPD.

pas au représentant de désigner pour lui-même un délégué à la protection des données.

CHAPITRE 3. Quel profil pour la fonction du délégué à la protection des données ?

SECTION 1. – Compétences requises

25. La notion de délégué à la protection des données n'est pas définie. On comprend à la lecture du profil associé à celui-ci et des missions dévolues à ce dernier dans le RGPD qu'il s'agit de s'adjoindre les services d'un spécialiste de la protection des données qui viendra contrôler en interne le respect de la législation et conseiller le responsable du traitement et le sous-traitant qui l'auront nommé en matière de protection des données. En revanche, le délégué à la protection des données n'a pas de fonction décisionnelle en ce sens qu'il revient au responsable du traitement ou sous-traitant pour lequel il exerce sa fonction de prendre les décisions en matière de traitement de données. Ainsi, une ligne de partage se dessine entre, d'une part, une série d'initiatives qu'un délégué à la protection des données peut/doit prendre pour remplir ses missions pour analyser, contrôler, conseiller et, d'autre part, les décisions qui sont prises concernant la mise en œuvre ou non d'un traitement, la réalisation ou non d'une analyse de risques, etc., qui doivent être prises par le responsable du traitement ou le sous-traitant. Nous y reviendrons dans la section relative aux responsabilités⁵⁶.

26. Les missions dévolues au délégué et définies dans le RGPD sont de plusieurs ordres et induisent indirectement les exigences de compétence pour les exercer.

Le RGPD prévoit par ailleurs que « le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39 »⁵⁷. Le Groupe 29 rattache la dimension « qualité

⁵⁶ Voy. *infra*, Section 6.

⁵⁷ Art. 37, 5°, du RGPD.

professionnelles » aux connaissances et à l'expérience de la personne présente pour exercer la fonction de DPO⁵⁸.

L'article 39 du RGPD prévoit que les missions assignées au délégué à la protection des données sont au moins les suivantes :

- « a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données ;
- b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;
- c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 ;
- d) coopérer avec l'autorité de contrôle ; ».

Ces missions impliquent tout d'abord, outre une bonne connaissance du secteur d'activités du responsable du traitement ou du sous-traitant par le délégué à la protection des données, une maîtrise de la législation en matière de protection des données, que ce soit au niveau du droit de l'Union ou du droit interne susceptible de s'appliquer au traitement des données. Cela peut laisser penser que le profil de juriste est sans doute privilégié. Pourtant, il nous semble que cela ne va pas de soi. La maîtrise des contingences et réalités techniques est également une dimension primordiale des compétences qu'un délégué à la protection des données devrait posséder. L'empreinte technologique est davantage prise en compte dans le RGPD qui tend à réguler des pratiques existantes (dont indéniablement le profilage lié au « *big data* ») notamment pour en évaluer les risques. On pense à l'analyse de risques, analyse qui comporte un volet technique. La mise en œuvre des principes de protection par défaut (*privacy by default*) et de protection dès la conception (*privacy by design*) impliquent également une bonne compréhension des aspects techniques liés aux ressources informatiques utilisées. Notons encore que le RGPD érige également en

⁵⁸ Lignes directrices (voy. *supra*, note n° 7), p. 11. La capacité à exercer la fonction doit s'apprécier au regard de son intégrité et sens de l'éthique ainsi qu'au regard de sa position dans l'organisation.

principe clé de la réglementation, celui de l'intégrité et la confidentialité qui impose au responsable du traitement de « garantir » la sécurité des données⁵⁹. Or assurer le respect de ce principe passe nécessairement par une maîtrise de la compréhension des risques techniques à rencontrer, fût-ce dans le rôle d'analyse, de contrôle et de conseil qui doit être celui du DPO. Il s'agit là à notre sens d'un aspect essentiel de la protection.

Les missions du délégué à la protection des données incluent également une dimension « éducative ». Il s'agit de s'assurer que le personnel du responsable du traitement ou le sous-traitant au service duquel il se trouve, est (in)formé en ce qui concerne l'application de la protection des données. Cette exigence se retrouve à la croisée de deux missions du délégué : celle de conseil et d'information et celle de contrôle. Il ne s'agit donc pas uniquement de conseiller le management mais de s'assurer que l'information passe également auprès des personnes qui, au jour le jour, participent à la mise en œuvre de traitements de données. L'idée est que le délégué à la protection des données puisse, au travers de l'exercice de ces compétences, insuffler une conscientisation au sein de l'entreprise en matière de prise en compte de la protection des données.

27. Par ailleurs, non seulement le délégué à la protection des données doit pouvoir conseiller mais il doit également contrôler le respect du RGPD. Il s'agit là d'une véritable gageure. Un des points sans doute les plus compliqués à gérer en matière de protection des données est d'avoir une vue de ce qui se passe dans une organisation en matière de traitements. Dès lors que tout est pratiquement informatisé, les initiatives de tous bords prises par l'un ou l'autre département impliquent potentiellement un traitement de données. Cartographier les traitements opérés et contrôler le respect des règles en matière de protection des données s'apparente bien souvent à de l'audit. Une autre dimension de la mission du délégué. À cet égard, le Groupe 29 ajoute que les missions confiées à l'article 39 au délégué constituant un minimum, il est loisible au responsable du traitement ou au sous-traitant de confier au délégué la tâche de réaliser et de mettre à jour le registre des activités de traitement visé à l'article 30 du RGPD⁶⁰. Cela pourrait lui permettre de conserver précisément une vue sur les traitements réalisés au sein de l'organisation.

28. Enfin, pour ce qui concerne le rôle de point de contact des personnes concernées et de l'autorité de contrôle, on touche là à des compétences de gestion de communication et de plaintes potentielles. N'entre

⁵⁹ Art. 5, § 1^{er}, du RGPD.

⁶⁰ Lignes directrices (voy. *supra*, note n° 7), p. 18.

toutefois pas nécessairement dans sa mission le traitement de plaintes ensuite : le relais peut être donné à un autre service, le cas échéant.

29. Bref, on peut se demander si toutes ces compétences sont aisées à rassembler en une seule personne. Une solution serait de fédérer ces compétences autour d'une équipe pluridisciplinaire. L'idée de désigner plusieurs délégués qui se répartissent les missions ou une personne morale avec du personnel regroupant ces compétences offrirait une solution.

Les Lignes directrices du Groupe 29 laissent la porte ouverte à de telles possibilités. Tout d'abord, comme nous l'avons évoqué, le Groupe précise que le contrat de services qui pourrait être conclu avec un tiers pourrait concerner soit une personne physique, soit une personne morale. Cela implique qu'on pourrait donc conclure un contrat pour des services de délégué à la protection des données avec une société de consultance qui mettrait à disposition du responsable du traitement ou du sous-traitant une équipe plutôt qu'une personne physique seule pour exercer cette compétence. Le Groupe semble suggérer que, dans ce cas, toutes les personnes physiques constituant l'équipe aient un statut se calquant sur celui de délégué à la protection des données. Chaque membre de l'équipe devrait disposer des compétences requises, ne pas avoir de conflit d'intérêts et être protégé contre une rupture du contrat liée à l'exercice non fautif de sa mission⁶¹. On suppose dès lors que ce seront ces personnes plutôt que la personne morale qui seront désignées comme délégués à la protection des données.

Il conviendra également d'identifier qui dans l'équipe est en charge de quelle(s) missions(s)⁶² et que l'une d'entre elle soit désignée comme personne de contact (« *lead contact* ») pour le client⁶³.

Par ailleurs, le Groupe évoque l'idée de permettre à un délégué à la protection des données employé dans les liens d'un contrat de travail de disposer d'une équipe au sein de laquelle les tâches et responsabilités de chacun des membres soient clairement définies⁶⁴. Sans aller jusqu'à exiger que chacune des personnes de l'équipe endosse la fonction de délégué à la protection des données, cela peut répondre à la préoccupation de pouvoir effectivement pendre en charge les différents aspects de la mission de délégué à la protection au travers d'une équipe.

30. Pour ce qui est du niveau d'expertise, le considérant n° 97 du RGPD précise que « le niveau de connaissances spécialisées requis devrait

⁶¹ Lignes directrices (voy. *supra*, note n° 7), p. 12.

⁶² Lignes directrices (voy. *supra*, note n° 7), p. 14.

⁶³ Lignes directrices (voy. *supra*, note n° 7), pp. 12 et 14.

⁶⁴ Lignes directrices (voy. *supra*, note n° 7), p. 14.

être déterminé notamment en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données à caractère personnel traitées par le responsable du traitement ou le sous-traitant ». Il s'agit donc d'une appréciation au cas par cas. Le Groupe 29 donne pour exemple de facteurs à prendre en compte, le fait qu'il s'agit de traitements complexes, qui portent sur un grand volume de données sensibles, ou encore qui concernent des transferts hors de l'Union européenne⁶⁵.

SECTION 2. – Absence de conflit d'intérêts

31. Le RGPD exige que « le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts »⁶⁶.

Il nous semble que le respect de cette obligation, gage d'une indépendance dans l'exercice des missions qui lui sont confiées, a des implications différentes selon que le délégué à la protection des données est désigné au sein du personnel du responsable du traitement ou du sous-traitant ou qu'il est fait appel à un « externe ».

En effet, telle que formulée, l'obligation fait peser sur le responsable du traitement ou sous-traitant employeur l'obligation de préserver le délégué de tout conflit d'intérêts en veillant à ne pas lui confier une autre fonction qui le placerait dans un tel conflit. Le RGPD prévoit en effet que le délégué à la protection des données peut exercer d'autres fonctions⁶⁷.

Un conflit d'intérêts pourrait exister lorsque la même personne est susceptible de devoir être contrôleur et contrôlé. Tel pourrait être le cas pour un responsable de projet qui exercerait une fonction de délégué à la protection des données alors qu'il serait, dans le cadre de cette fonction, amené à porter des projets impliquant le traitement de données à caractère personnel et, dans sa fonction de délégué à la protection des données, contrôler que cela est conforme à la réglementation. Il est en revanche *a priori* concevable de confier la fonction de délégué à la protection des données à un juriste d'entreprise ou à un conseiller technique. Cette fonction ne pourrait toutefois être assumée par des personnes qui seront amenées à déterminer les finalités et moyens de traitement des données traitées dans l'organisation⁶⁸. Si la règle paraît claire et saine, elle peut s'avérer difficile

⁶⁵ Lignes directrices (voy. *supra*, note n° 7), p. 11.

⁶⁶ Art. 38, § 6, du RGPD.

⁶⁷ Art. 38, § 6, du RGPD.

⁶⁸ Lignes directrices (voy. *supra*, note n° 7), p. 16.

à apprécier en pratique. Tout membre du personnel peut être amené à gérer des traitements de données au sein de l'organisation : le juriste qui gère des dossiers contentieux, le responsable des ressources humaines qui est à la manœuvre pour les traitements de données relatifs aux employés, etc. Un élément déterminant pourrait être le pouvoir décisionnel ou non qu'a le délégué à la protection des données dans l'exercice de son autre fonction. En ce sens, le Groupe 29 mentionne une série de fonctions qui ne serait *a priori* pas compatibles avec la fonction de délégué à la protection des données et qui ont en commun d'être celles de dirigeants de l'entreprise ou de départements d'une organisation (directeur du service informatique, des ressources humaines, du marketing, etc.)⁶⁹.

Un autre cas de figure est celui du délégué à la protection des données désigné par contrat de service et qui est extérieur à l'organisation. L'absence de conflit d'intérêts peut être liée aux tâches confiées (un délégué intervenant comme consultant mais qui serait sollicité pour d'autres missions au sein de l'organisation du responsable du traitement ou du sous-traitant, un avocat qui agirait comme délégué à la protection des données et qui ne pourrait défendre l'entité en justice sur ces questions), aux clients d'une personne morale qui auraient des intérêts opposés, mais également à la situation du tiers par rapport par exemple à une autorité de contrôle. On imagine mal une personne siégeant dans une autorité de contrôle intervenir comme délégué à la protection des données dans une quelconque organisation.

CHAPITRE 4. Quelles sont les particularités de la fonction et du statut juridique du délégué à la protection des données ?

SECTION 1. – Statut de salarié ou d'indépendant

32. L'article 37, 6°, du RGPD prévoit que « [l]e délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service ».

Un délégué à la protection des données peut donc exercer sa fonction en qualité d'employé ou d'indépendant. Comme expliqué ci-avant, une

⁶⁹ Lignes directrices (voy. *supra*, note n° 7), p. 16.

personne morale peut, selon le Groupe 29, être désignée comme délégué à la protection des données⁷⁰.

Le RGPD n'interfère *a priori* pas avec les règles nationales régissant les particularités des contrats concernés, notamment sur les conditions de forme des contrats ainsi que sur le régime juridique applicable, tel celui de la responsabilité⁷¹, sauf sur certains points détaillés dans les sections suivantes.

SECTION 2. – Exigence d'une forme d'indépendance

33. Tout d'abord, le RGPD impose une forme d'indépendance dont doit bénéficier le délégué à la protection des données dans l'exercice de sa mission⁷².

L'article 38, paragraphe 3, du RGPD prévoit que « Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions ». Ce principe vient heurter celui du lien de subordination, caractéristique en droit belge du contrat de travail et dont découlent les prérogatives patronales de pouvoir donner des instructions à un travailleur.

À notre sens, il faut circonscrire ce que recouvre cette « indépendance » de l'exercice des missions dévolues aux DPO. Cela ne concerne pas les instructions générales qui peuvent être données à un membre du personnel concernant le cadre de travail, telles qu'on les retrouve dans le règlement de travail par exemple, ou encore des consignes de sécurité ou des indications concernant l'usage de l'outil informatique. L'esprit du règlement est que le délégué à la protection des données ne reçoive pas d'instruction concernant la manière de réaliser ses missions (comment répondre à une plainte, quels contrôles effectuer, quelles appréciations faire concernant la légalité d'un traitement et, précise le Groupe 29, si le délégué à la protection des données devrait ou non consulter l'autorité de contrôle sur une question)⁷³. L'idée est donc que le délégué à la protection des données puisse le cas échéant faire des constats qui dérangent, ou donner des conseils qui n'arrangent pas le responsable du traitement ou

⁷⁰ Voy. *infra*, *supra*, Chapitre 3, Section 2, et Lignes directrices (voy. *supra*, note n° 7), p. 12.

⁷¹ Voy. *infra*, Section 6.

⁷² Cette exigence d'indépendance est également rappelée dans le considérant n° 97 du RGPD.

⁷³ Lignes directrices (voy. *supra*, note n° 7), p. 15.

le sous-traitant. En revanche, le délégué à la protection des données peut évidemment recevoir des demandes spécifiques du responsable du traitement ou sous-traitant qui fait appel à ses services. Ainsi lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement a-t-il même l'obligation de demander conseil au délégué à la protection des données⁷⁴.

34. Par ailleurs, on peut imaginer qu'un employé cumule la fonction de DPO avec une autre fonction, telle celle de juriste d'entreprise, et qu'il puisse se voir donner des instructions concernant les tâches lui incombant en tant que juriste d'entreprise et non quant à celles qui relèvent de la fonction de DPO.

Le corollaire de cette exigence théorique d'indépendance est que le délégué à la protection des données dispose des ressources et du temps nécessaire pour exercer effectivement ses missions. C'est un aspect de la dynamique de collaboration avec le responsable du traitement ou le sous-traitant prévue dans le RGPD⁷⁵ et qui est d'ailleurs souligné par le Groupe 29. Ces ressources seront différentes selon que l'on se trouve ou non dans le cas de figure d'une relation salariée.

35. Pour reprendre les exigences dégagées par le Groupe 29 dans les Lignes directrices du 13 décembre 2016⁷⁶, certaines nous semblent s'appliquer davantage au cas d'un « *DPO in house* » : un soutien du haut management, des ressources matérielles (ou de personnel selon l'importance et la complexité des activités de traitements), des possibilités de suivre des formations pour suivre les développements en matière de protection des données, ou encore dans le cas où un DPO cumule plusieurs fonctions, une organisation de la charge de travail qui lui permette d'exercer ses fonctions de DPO. Les autres formes de support au délégué à la protection des données sont pertinentes dans tous les cas de figure : diffusion en interne de l'identité et du rôle du délégué à la protection des données et accès aux différents services pour recevoir les informations nécessaires à l'exercice de la mission⁷⁷.

36. Enfin, le RGPD prévoit spécifiquement que le délégué à la protection des données « fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant »⁷⁸. Dans le

⁷⁴ Art. 35, § 2, du RGPD.

⁷⁵ Art. 38, § 2, du RGPD.

⁷⁶ Lignes directrices (voy. *supra*, note n° 7), p. 14.

⁷⁷ Lignes directrices (voy. *supra*, note n° 7), p. 14.

⁷⁸ Art. 38, § 3, du RGPD.

cadre d'une relation de contrat de travail, cela oblige donc à considérer la fonction de DPO en dehors d'une ligne hiérarchique. Toutefois, sur le plan des canaux de communication à privilégier, le texte n'est pas des plus clairs. À notre sens, cela n'implique pas que le délégué à la protection des données ne puisse s'adresser ou faire part de son opinion à d'autres membres de l'organisation concernée. En effet, dans la mission d'information il pourrait être amené à répondre à des interpellations, à donner des conseils, sans qu'on imagine que la direction joue l'intermédiaire pour toutes ces communications. Il conviendra sans doute de distinguer les communications qui peuvent avoir une portée sur une décision à prendre par le responsable du traitement ou le sous-traitant, et celles qui s'inscrivent dans un autre contexte.

SECTION 3. – Protection contre des « représailles »

37. Toujours dans l'objectif de garantir une liberté d'action du délégué à la protection des données, le RGPD prévoit que ce dernier « ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions »⁷⁹.

Le Groupe 29 envisage les pénalités au sens large. Il s'agit de toute conséquence ou menace de conséquence négative sur l'évolution de la carrière, la rémunération, le renouvellement d'un contrat qui interviendrait pour un motif lié à l'exercice des missions du délégué à la protection des données, et pas uniquement la rupture d'un contrat⁸⁰. La rupture de contrat devrait inclure également à notre sens l'hypothèse où un employeur envisage de modifier la fonction du délégué à la protection des données pour lui retirer ses missions, tout en le conservant à son service pour d'autres fonctions⁸¹.

38. La difficulté de ce genre de situation est de démontrer que la décision critiquée est ou non liée à l'exercice de la mission. Le RGPD ne prévoit pas de règles en ce qui concerne la charge de la preuve⁸², comme c'est le cas

⁷⁹ Art. 38, § 3, du RGPD.

⁸⁰ Lignes directrices (voy. *supra*, note n° 7), pp. 14-15.

⁸¹ En droit belge, cela rejoint la problématique du *ius variandi* et de la modification unilatérale d'un élément essentiel du contrat de travail. Voy. à ce sujet, V. VANNES et L. DEAR, « Titre 2 – La modification des éléments essentiels du contrat de travail et l'abus de droit », in *La rupture abusive du contrat de travail*, Bruxelles, Bruylant, 2010, pp. 563-577.

⁸² Sauf à considérer que le principe d'*accountability* impose, à tout le moins pour ce qui concerne le responsable de traitement, de prouver qu'il a respecté ses obligations en la matière et que la sanction prise à l'encontre d'un délégué n'est pas une mesure de rétorsion en réaction à une position prise par le délégué dans l'exercice de sa mission.

généralement dans le cadre de mécanismes de protection contre le licenciement⁸³. Cela peut être inconfortable pour les deux parties. Il sera difficile pour le délégué à la protection des données d'introduire une plainte au sein de l'entreprise ou devant un tribunal en cours de contrat pour réclamer une promotion ou une augmentation, sans compter que le délégué à la protection des données est lié par une obligation de confidentialité concernant l'exercice de ses missions. L'employeur devra quant à lui pouvoir justifier les décisions qu'il prend à l'égard du délégué à la protection des données et serait avisé de redoubler de prudence pour établir qu'elles sont sans lien avec l'exercice de la mission du délégué. On ne peut que conseiller de baliser au mieux les conditions d'évolution de carrière et de rémunération ainsi que les modalités d'octroi des droits à des ressources de travail (véhicule de fonction, etc.) afin d'objectiver les décisions prises à cet égard.

39. Reste un point délicat : on peut se demander si on pourra licencier ou mettre fin à un contrat de services conclu avec un DPO médiocre. La question peut choquer mais dès lors qu'on ne peut pas donner d'instruction ni contrôler le délégué à la protection des données, comment justifier la mise à pied d'un prestataire qui se révèle incompetent ? Dans ses Lignes directrices, le Groupe 29 envisage des hypothèses de licenciement uniquement pour des circonstances tout à fait étrangères à l'exercice des missions (vol, harcèlement sexuel ou moral ou dans un cas de faute grave du même ordre)⁸⁴. Mais *quid* du manque de proactivité, d'erreurs d'appréciation dans le chef du délégué à la protection des données ? La question reste ouverte⁸⁵, mais il est prudent de solliciter de rapports d'activités et des avis écrits du délégué pour pouvoir objectiver les problèmes dans la qualité des prestations qui seraient rencontrés, le cas échéant⁸⁶.

⁸³ Par exemple en cas de dépôt de plainte pour harcèlement, ou de protection du licenciement de la femme enceinte, du travailleur délégué syndical, etc. Voy. à ce sujet, K. ROSIER, S. GILSON et E. DERMINE, « La preuve en droit du travail », in *La preuve : questions spéciales*, CUP, vol. 99, Louvain-la-Neuve, Anthemis, 2007, pp. 206 et s.

⁸⁴ Lignes directrices (voy. *supra*, note n° 7), p. 16.

⁸⁵ Notons qu'en droit belge dans un arrêté royal du 6 décembre 2015 (et donc antérieur à l'adoption du RGPD), qui encadre le fonction de conseillers en sécurité et en protection de la vie privée dans les zones de police, il expressément prévu que « L'employeur ou l'autorité compétente ne peut rompre le contrat du conseiller, mettre fin à l'occupation statutaire du conseiller ou l'écarter de sa fonction que pour des motifs qui sont étrangers à son indépendance ou pour des motifs qui démontrent qu'il est incompetent à exercer ses missions » (art. 6 de l'arrêté royal du 6 décembre 2015 relatif aux conseillers en sécurité et en protection de la vie privée et à la plate-forme de la sécurité et de la protection des données). La question de la compétence est donc abordée et, de la formulation du texte, on peut déduire que l'employeur aura la charge de la preuve des motifs du licenciement.

⁸⁶ Il s'agit d'ailleurs d'une recommandation reprise dans une version amendée des Lignes directrices, p. 15.

SECTION 4. – Obligation de confidentialité

40. L'article 38, paragraphe 5, du RGPD prévoit que « Le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres ».

Il est donc essentiellement renvoyé sur ce point au droit national. Nous supposons que cela implique que soit le délégué à la protection des données sera soumis à une obligation de secret professionnel ou de confidentialité de par l'application de la loi nationale, soit qu'il appartiendra de prévoir une obligation de confidentialité dans son chef dans son contrat si tel n'est pas le cas, le tout en tenant compte des règles de droit interne. On suppose par ailleurs, que la portée et les limites aux obligations de secret ou de confidentialité dépendront et seront à interpréter au regard du droit national.

41. Dans ses Lignes directrices, le Groupe 29 précise uniquement que, selon lui, cette obligation de secret ou de confidentialité ne devrait pas empêcher le délégué à la protection des données de solliciter un avis auprès de l'autorité de contrôle nationale⁸⁷. On ajoutera que ce dernier ne peut évidemment pas se retrancher derrière une obligation de secret ou de confidentialité pour se dérober aux obligations qui lui sont imposées dans le RGPD. Ainsi, le RGPD prévoit-il que les personnes concernées peuvent prendre contact avec le DPO « au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le [...] règlement »⁸⁸. Cela implique que le délégué soit habilité à répondre à ces questions.

SECTION 5. – Descriptif des missions du délégué à la protection des données

42. Les fonctions énoncées à l'article 39 du RGPD sont les missions minimales incombant au délégué à la protection des données. Le Groupe 29 considère que les missions confiées à l'article 39 au délégué constituant un minimum, il est loisible au responsable du traitement ou au

⁸⁷ Lignes directrices (voy. *supra*, note n° 7), p. 18.

⁸⁸ Art. 38, § 4, du RGPD.

sous-traitant de lui confier d'autres tâches⁸⁹. Il évoque par exemple la tâche de réaliser et de mettre à jour le registre des activités de traitement visé à l'article 30 du RGPD. Cela pourrait lui permettre de conserver précisément une vue sur les traitements réalisés au sein de l'organisation.

Le Groupe 29 préconise de préciser dans les missions du délégué quelles seront ses tâches dans le cadre de la préparation d'une analyse d'impact et dans la mise en œuvre de celle-ci, et d'assurer une communication de ces missions en interne, aux employés ou intervenants concernés par les questions de protection des données⁹⁰.

SECTION 6. – Considérations méthodologiques

43. Enfin, élément singulier, le RGPD formule une exigence d'ordre méthodologique dans la manière dont le délégué est censé exercer sa mission. L'article 39, paragraphe 2, précise que « Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement ». Le Groupe 29 traduit cette consigne comme commandant une approche orientée sur le risque, devant permettre au délégué de définir les priorités dans tous les aspects de ses missions, et ce notamment dans le choix des traitements qui méritent davantage d'attention quant aux actions à prendre⁹¹.

Il convient toutefois de garder à l'esprit que les décisions relatives à des traitements, au regard des risques identifiés, n'incombent pas au délégué à la protection des données. De telles décisions relèvent du management, ou le cas échéant d'un département de « *risk management* » dédié comme en connaissent certaines entreprises.

⁸⁹ Lignes directrices (voy. *supra*, note n° 7), p. 19.

⁹⁰ Lignes directrices (voy. *supra*, note n° 7), p. 17.

⁹¹ Lignes directrices (voy. *supra*, note n° 7), p. 17.

CHAPITRE 5. Quelles sont les obligations du responsable du traitement ou du sous-traitant liées à la désignation du délégué à la protection des données ?

44. Outre l'obligation de mettre à disposition les ressources nécessaires que nous avons décrites sous le chapitre 4, section 2 *supra*, le responsable du traitement ou le sous-traitant qui désigne un délégué à la protection des données est soumis à des obligations particulières

SECTION 1. – Publicité de la fonction

45. Le premier objectif derrière cette exigence est d'assurer la transparence concernant cette désignation.

L'article 37, paragraphe 7, du RGPD prévoit à cet égard que « [l]e responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle ».

La disposition comporte donc deux volets. Le premier concerne la publication des coordonnées du délégué. Le texte ne précise pas quelles informations sont à communiquer ni, en pratique, sur quel support doit intervenir cette publication. Le second volet de la disposition prévoit une communication spécifique à l'autorité de contrôle, sans que la forme que doit prendre cette notification ne soit pas non plus spécifiée.

46. Aux termes d'une analyse téléologique de la disposition, le Groupe 29 préconise que soient communiquées les informations nécessaires pour pouvoir contacter *directement* le délégué, sans avoir à passer par un autre service. L'enjeu est également d'encourager des prises de contact avec le délégué, un contact direct et sous le sceau de la confidentialité étant de nature à rassurer les interlocuteurs⁹². La communication de l'identité du délégué aux tiers à l'organisation est laissée à l'appréciation du responsable du traitement ou sous-traitant. Le Groupe estime en revanche qu'il est souhaitable de définir des canaux de communication dédiés (au

⁹² Lignes directrices (voy. *supra*, note n° 7), p. 12.

minimum une adresse postale, adresse mail et numéro de téléphone attaché à la fonction ; le Groupe évoque aussi des moyens de contacts additionnels adaptés au media utilisé pour informer les tiers, tel un formulaire de contact sur un site web, etc.) et de communiquer au public les informations permettant cette prise de contact directe et effective⁹³. Un moyen aisé de réaliser cette communication serait de la publier sur le site internet de l'organisation si un tel site existe. Pour ce qui est de la communication en interne, le Groupe 29 indique que le nom et les données de contact devraient être communiqués, par exemple, via un intranet⁹⁴.

47. Il est à noter que, parallèlement à ces obligations de publication et de transparence⁹⁵, d'autres dispositions imposent des communications spécifiques. On constate à cet égard une constante (les informations minimales à fournir au titre de coordonnées ne sont pas précisées), et des disparités quant à l'obligation d'indiquer ou non l'identité du délégué⁹⁶.

SECTION 2. – Implication du délégué à la protection des données dans les questions de protection des données

48. Nous avons indiqué dans l'introduction de cette contribution que la désignation d'un délégué à la protection des données n'était qu'une première étape sur le chemin du respect de la réglementation. Une telle désignation demeurerait stérile si le délégué n'avait pas la possibilité d'exercer effectivement les missions qui lui sont dévolues. Cela passe par un accès aux services et aux informations utiles, comme rappelé ci-avant⁹⁷. Le RGPD exige en outre une certaine proactivité du responsable du traitement ou du sous-traitant qui a désigné le délégué.

⁹³ Lignes directrices (voy. *supra*, note n° 7), p. 13.

⁹⁴ Lignes directrices (voy. *supra*, note n° 7), p. 13.

⁹⁵ À noter également, l'obligation de faire figurer les noms et coordonnées du délégué à la protection des données dans le registre de traitement (art. 30 du RGPD).

⁹⁶ Les coordonnées du délégué à la protection des données comptent parmi les informations à fournir à la personne concernée lors de la collecte d'informations (voy. art. 13 et 14 du RGPD). Par ailleurs, il est fait obligation au responsable du traitement de communiquer les coordonnées du DPO en cas de consultation préalable de l'autorité de contrôle intervenant au terme de la réalisation d'une analyse d'impact (art. 36, § 3, d), du RGPD). Lorsqu'une notification de violation de données, on exige cette fois la communication à l'autorité de contrôle non seulement des coordonnées du délégué mais également son identité (art. 33, § 2, b), du RGPD).

⁹⁷ Voy. Chapitre 4, Section 2, *supra*.

L'article 38, paragraphe 1^{er} du RGPD prévoit que « Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ».

49. Pour ce qui concerne l'implication dans toutes les questions qui sont liées à la protection des données, cela peut se faire à la fois sur le plan organisationnel (intégration du délégué à la protection des données à des équipes de projet ou groupes de travail, par exemple), et/ou dans le cadre des processus décisionnels (consultation préalable du délégué lors de la prise de décision, la conclusion de contrats avec des sous-traitants, etc.). Sur ce dernier point, le Groupe 29 évoque l'idée de développer des lignes de conduite en interne mettant en évidence dans quels cas de figure il convient de consulter le délégué à la protection des données, qu'il s'agisse de démarches préventives (assurer par exemple le respect du principe de protection dès la conception d'un projet)⁹⁸ ou curatives (prendre les mesures nécessaires en cas de violation de données à caractère personnel⁹⁹)¹⁰⁰.

Un cas est, par ailleurs, spécifiquement abordé dans le RGPD qui oblige, d'une part, le responsable du traitement ou sous-traitant à prendre avis auprès du délégué à la protection des données et, d'autre part, le délégué à conseiller ces derniers. Il s'agit du délicat exercice de l'analyse d'impact¹⁰¹. Le Groupe 29 recommande que le responsable du traitement ou sous-traitant définisse clairement sur quels points le délégué à la protection des données doit être consulté concernant la nécessité, la mise en œuvre et la validation des analyses de risques¹⁰².

CHAPITRE 6. Comment se répartissent les responsabilités des différents protagonistes ?

50. Alors que l'accent est clairement mis sur la responsabilité des différents intervenants dans les traitements de données, qu'il s'agisse des responsables du traitement, des sous-traitants ou encore des représentants, le RGPD ne dit pas un mot de la responsabilité du délégué à la protection des données.

⁹⁸ Art. 25 du RGPD.

⁹⁹ Art. 33 du RGPD.

¹⁰⁰ Lignes directrices (voy. *supra*, note n° 7), p. 14.

¹⁰¹ Art. 35, § 2 et 39, § 1^{er}, c), du RGPD.

¹⁰² Lignes directrices (voy. *supra*, note n° 7), pp. 17-14.

Dans ses Lignes directrices, le Groupe 29 souligne le fait que seul le responsable du traitement ou le sous-traitant est responsable des manquements en matière de protection des données¹⁰³. La raison en est que le pouvoir décisionnel en cette matière appartient à ces derniers, et non au délégué à la protection des données.

Les avis, conseils, recommandations donnés par le délégué ne sont pas obligatoires ni contraignants. Si le Groupe 29 insiste sur le poids à donner à l'opinion du délégué à la protection des données par le responsable du traitement ou le sous-traitant, il n'exclut pas un désaccord. Il invite dans ce cas le responsable ou sous-traitant à documenter les motifs pour lesquels l'avis du délégué n'est pas suivi, et ce toujours dans l'esprit du principe d'*accountability*¹⁰⁴.

On en déduit donc que le responsable du traitement ou le sous-traitant ne peut se dédouaner de sa responsabilité en rejetant la faute sur le délégué à la protection des données. La question de la responsabilité du délégué à la protection des données vis-à-vis du responsable du traitement ou du sous-traitant est-elle pour autant évacuée ? On peut imaginer des erreurs ou carences graves dans l'exercice de la mission, non imputables au responsable du traitement, et qui devraient pouvoir être sanctionnées dès lors qu'on ne peut être totalement immunisé de toute faute, nous semble-t-il. Au vu des règles énoncées et des premières interprétations faites par le Groupe 29, il est difficile de tirer des conclusions claires à ce sujet, d'autant que, comme expliqué *supra*, on ne peut pas sanctionner un délégué pour un motif lié à l'exercice de sa fonction...

À supposer qu'on puisse concevoir une mise en cause de la responsabilité du délégué, nonobstant les limites que nous venons de rappeler, il conviendra d'avoir égard au régime juridique propre au statut du délégué. Celui-ci peut différer par exemple, selon qu'on a affaire à un salarié dont la responsabilité peut être limitée par l'effet de la loi, ou à un prestataire indépendant pour lequel de telles limites n'existent pas automatiquement et dont la responsabilité peut être *a priori* plus largement engagée.

¹⁰³ Lignes directrices (voy. *supra*, note n° 7), p. 4.

¹⁰⁴ Lignes directrices (voy. *supra*, note n° 7), p. 13.

CHAPITRE 7. Qu'en est-il des autres personnes chargées de la protection des données ?

51. Il reste possible à l'organisation de confier à une personne interne ou externe à l'entreprise des tâches en lien avec la protection des données à caractère personnel sans lui assigner la fonction de délégué à la protection des données. Dans ce cas, le Groupe 29 préconise d'éviter toute confusion à l'égard du public ou en interne quant au statut de cette personne, à ses missions et tâches réelles, notamment en évitant de lui attribuer le titre de délégué à la protection des données. Il conviendra de privilégier une autre dénomination de fonction¹⁰⁵.

La question se pose de savoir si on peut simplement disqualifier une fonction, c'est-à-dire confier à une personne les missions du délégué à la protection des données tout en donnant un autre titre pour échapper aux contraintes liées à l'organisation de la fonction. L'esprit du texte du RGPD est de ne permettre à un responsable du traitement ou à un sous-traitant de se prévaloir de la désignation d'un délégué à la protection des données que s'il met en place les garanties d'indépendance qui doivent y être associées¹⁰⁶. Le texte protège donc davantage la fonction, qui ne peut être galvaudée, que les personnes qui l'occupent. Ceci dit, l'intérêt principal du titre de délégué à la protection des données pour celui qui occupe la fonction est une protection contre la rupture de contrat pour des motifs liés à l'exercice de sa fonction dans laquelle il pourrait être amené à dénoncer des irrégularités ou préconiser des solutions qui n'iraient pas dans le sens des intérêts commerciaux de la société qui a recours à ses services. Rien n'empêche, en droit belge, un travailleur d'invoquer le caractère abusif ou déraisonnable de son licenciement si celui-ci intervient pour un motif lié à l'exercice non critiquable de sa fonction, même si celui-ci n'a pas la même fonction de DPO.

¹⁰⁵ Lignes directrices (voy. *supra*, note n° 7), pp. 5 et 6.

¹⁰⁶ Évoquées sous le Chapitre 4, Section 2, *supra*.

CHAPITRE 8. Quelles sont les sanctions encourues en cas du non-respect de leurs obligations pour ceux qui désignent ou doivent désigner un délégué à la protection des données ?

52. En vertu de l'article 83, paragraphe 4, du RGPD, l'autorité de contrôle peut imposer une amende administrative pouvant s'élever jusqu'à 10.000.000 euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu en cas de non-respect des obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 37 à 39.

53. Nous ne détaillerons pas, dans le cadre de la présente contribution, la manière dont ces sanctions vont être appliquées et les éléments que le RGPD met en exergue pour guider l'autorité de contrôle dans l'appréciation de l'ampleur de la sanction à adopter. Nous nous contenterons de souligner que toute violation des dispositions précitées est susceptible d'être sanctionnée. Il ne s'agit donc pas *a priori* uniquement de l'absence de désignation d'un délégué alors qu'un responsable du traitement ou un sous-traitant en avait l'obligation, mais également le fait par exemple que ces derniers ne respectent pas les obligations qui leur incombent pour permettre au délégué d'exercer sa mission de manière effective et indépendante. Les sanctions nous paraissent donc applicables même dans l'hypothèse où un responsable de traitement ou sous-traitant n'avait pas initialement l'obligation de désigner un délégué à la protection des données.

Conclusions

54. Sur le principe, il nous apparaît que l'idée de prévoir la désignation d'un délégué à la protection des données est cohérente avec l'orientation prise dans le RGPD : davantage de responsabilisation dans la prise en compte de la protection des données. C'est au cœur de l'entreprise et des administrations que naissent les traitements de données et c'est au cœur de celles-ci que la protection des données doit être gérée au premier chef.

LE RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Face à une réglementation qui devient de plus en plus complexe et affaire de spécialistes (il suffit de s'attaquer à la lecture du règlement pour s'en convaincre...), contraindre ceux qui mettent en œuvre les traitements de données à s'adjoindre les services d'un spécialiste a tout son sens. Et on a dénoté une réactivité face aux changements qui s'annonçaient avec les recrutements de DPO et les formations *ad hoc* qui sont proposées sur le marché dès avant l'entrée en application du RGPD.

La mise en pratique n'est toutefois pas sans poser des difficultés et des questions. À l'heure où la fonction de DPO s'organise dans les entreprises et au sein des autorités, il reste beaucoup à définir. Outre les aspects pratiques de rédaction de contrats de travail (ou d'avenants) ou de contrat de services pour l'engagement d'un DPO, d'élaboration de procédures internes à créer, d'organigrammes de fonctions à revoir, c'est le « métier » de DPO au jour le jour qui suscite son lot de questionnements. Nous avons mis en évidence dans cette contribution quelques zones d'ombres qu'il reste à baliser. Le Groupe 29 a annoncé d'autres lignes directrices pour accompagner les acteurs. Il est également à espérer que les autorités de contrôle pourront fournir des indications lorsque les questions pratiques se poseront. Une partie de ces questions pourraient d'ailleurs naître de l'application du RGPD dans le contexte de la législation interne.

Nous concluons par ce constat : la fonction de DPO est encore à ce stade, une fonction *en devenir*.